REMARKS/ARGUMENTS

Claims 1-80 are pending in the present application.

This Amendment is in response to the Office Action mailed May 3. 2004. In the Office Action, the Examiner rejected claims 1-80 under 35 U.S.C. §101, second paragraph; claims 17-20, 37-40, 57-60, 77-80 under 35 U.S.C. §112; claims 1-5, 21-25, 41-45 and 51-65 under 35 U.S.C. §102(e); and claims 6-7, 8, 9-17, 26-27, 8, 29-37, 46-47, 48, 49-57, 66-67, 68 and 69-77 under 35 U.S.C. §103(a). Applicants have amended claims 1-3, 17-19, 21-23, 37-39, 41-43, 45-55, 57-59, 61,63, and 77-79. Reconsideration in light of the amendments and remarks made herein is respectfully requested.

Double Patenting 35 U.S.C. § 101

1. The Examiner rejects claims 1-80 under the judicially created doctrine of the obviousness-type double patenting of the claim of copending Application No. 09/541,667. The Examiner asserts that although the conflicting claims are not identical, they are not patentably distinct from each other. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented. However, in light of the amendments, Applicants request the provisional rejection be withdrawn.

Rejection Under 35 U.S.C. § 112

In the Office Action, the Examiner rejected claims 17-20, 37-40, 57-60, 77-80 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. Applicants respectfully disagree.

The Examiner states that the phrases "chipset isolated nub loader hash" and "chipset isolated hash log" are not clearly defined in the specification (Office Action, page 3 , paragraph 5). Applicants respectfully direct the Examiner's attention to the Specification, page 13 (lines 8-24), and page 18 (lines 11-19). However, to clarify the claim language, claims 17-19, 37-39, 57-59 and 77-79 have been amended.

Therefore, Applicants respectfully request the rejection under 35 U.S.C. §112 be withdrawn.

Rejection Under 35 U.S.C. § 102

1. In the Office Action, the Examiner rejected claims 1-5, 21-25, 41-45 and 51-65 under 35 U.S.C. §102(e) as being anticipated U.S. Patent No. 6,357,004 issued to Davis et al. ("Davis-004"). Applicants respectfully traverse the rejection and contend that the Examiner has not met the burden of establishing a prima facie case of anticipation. To anticipate a claim, the reference must teach every element of a the claim. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Vergegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the...claim." Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ 2d 1913, 1920 (Fed. Cir. 1989).

Davis-004 discloses a system and method for ensuring integrity throughout post-processing. A system includes a host processor and a manipulation processing element (Davis-004, col. 3, lines 58-63). The manipulation processing element comprises a device contained within a package (Davis-004, col. 4, lines 23-25). The device supports post-processing operations and cryptographic operations such as encryption and/or decryption, creation of a digital signature, performance of a hash function, and generation of keys (Davis-004, col. 4, lines 29-37). None of these elements corresponds to an isolated execution mode.

Davis-004 does not disclose, either expressly or inherently, (1) a digest memory to store an isolated digest, (2) a device to attest the isolated execution mode and prove validity of a program loaded into the isolated memory area, (3) a secure environment for an isolated execution mode, (4) a processor operating in one of a normal execution mode and the isolated execution mode, and (5) a communication storage to exchange security information with the processor in the isolated execution mode.

The Examiner states that Davis-004 discloses one processor having one of a normal execution mode and an isolated execution mode (Office Action, page 4, paragraph 6). Applicants respectfully disagree.

First, Davis-004 does not disclose a digest memory to store an isolated digest. As supported in the specification, the isolated digest acts like a fingerprint identifying a supervisory code involved in controlling the isolated execution configuration and operation. Davis-004

merely discloses a non-volatile memory element to store a device unique, public/private key pair to support public-key cryptography, at least one digital certificate, and software to support post-processing operations (Davis-004, col. 4, lines 48-52). None of these elements is equivalent to the isolated digest.

Second, Davis-004 does not disclose a device to attest the isolated execution mode and prove validity of a program loaded in the isolated memory area.

Third, Davis-004 discloses two separate processors: a host processor and a manipulation processing element, not a processor having two modes of operations. The memory unit accessible to the manipulation processing element is not accessible to the host processor (Davis-004, col. 4, lines 59-67).

Fourth, the manipulating processing element may perform post-processing and cryptographic operations, but not operations in an isolated execution mode. As supported in the Specification, the isolated execution mode includes configuration for isolated execution, definition of an isolated area, definition of isolated instructions, generation of isolated access bus cycles, and generation of isolated mode interrupts (See Specification, page 8, lines 22-25); page 9, lines 1-2). Claims should be interpreted consistently with the specification, which provides content for the proper construction of the claims because it explains the nature of the patentee's invention. See Renishaw, 158 F.3d 1250. Here, the meaning of the isolated execution mode must be interpreted consistently with the Specification.

Fifth, Davis-004 does not disclose communication storage to allow a device to exchange security information with the processor in the isolated execution mode. Davis-004 merely discloses that for authentication, digital signature may be accompanied by a digital certificate chain (Davis-004, col. 3, lines 14-16). There is no communication storage. The manipulation processing element merely performs post-processing operations on information after the information has been digitally signed (Davis-004, col. 3, lines 38-40). There is no attestation.

Therefore, Applicants believe that independent claims 1, 21, 41, 61 and their respective dependent claims are distinguishable over the cited prior art references. Accordingly, Applicants respectfully request the rejection under 35 U.S.C. §102(e) be withdrawn.

Rejection Under 35 U.S.C. § 103

1. In the Office Action, the Examiner rejected: (1) claims 6-7, 9-17, 26-27, 29-37, 46-47, 49-57, 66-67 and 69-77 under 35 U.S.C. §103(a) as being unpatentable over Davis-004 in view of U.S. Patent No. 4,319,323 issued to Ermolovich ("Ermolovich"), and (2) claims 8, 28, 48 and 68 under 35 U.S.C. §103(a) as being unpatentable over Davis-004 in view of Ermolovich and further in view of U.S. Patent No. 5,844,986 issued to Davis ("Davis-986").

Applicants respectfully traverse the rejection and contends that the Examiner has not met the burden of establishing a prima facie case of obviousness. As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *MPEP §2143, p. 2100-129 (8th Ed., rev. 2, May 2004).* Applicants respectfully contends that there is no suggestion or motivation to combine their teachings, and thus no *prima facie* case of obviousness has been established.

Davis-004 discloses a system and method for ensuring integrity throughout post-processing as discussed above.

Ermolovich discloses a communications device for data processing system. A device status is built and inserted into a packet as a status longword before inserting a command packet into a termination queue (Ermolovich, coo. 85, lines 37-41). The device status contains the status of a communication device after the communication device processes a command packet (Ermolovich, col. 13, lines 37-43). A command interpreter transfers contents of a command field to a command register in an external device (Ermolovich, col. 12, lines 2-6). The communication device may directly write to or read from buffers in the data block and command block (Ermolovich, col. 7, lines 54-58).

Davis-986 discloses a electronic system and method for controlling access through user authentication. In a field BIOS upgrade, a software manufacturer (the BIOS vendor) sends the user a diskette containing a new BIOS code (Davis-986, col. 3, lines 38-40). An authentication is performed to ensure that the revision date is appropriate (Davis-986, col. 4, lines 7-15).

Davis-004, Ermolovich and Davis-986, taken alone or in any combination, does not disclose, suggest, or render obvious (1) a digest memory to store an isolated digest, (2) a device to attest the isolated execution mode and prove validity of a program loaded into the isolated memory area, (3) a secure environment for an isolated execution mode, (4) a processor operating in one of a normal execution mode and the isolated execution mode, and (5) a communication storage to exchange security information with the processor in the isolated execution mode. There is no motivation to combine Davis-004, Ermolovich and Davis-981 because none of them addresses the problem of isolated execution. There is no teaching or suggestion that a digest memory, a device to attest isolated execution mode, and a processor having normal and isolated execution modes is present. Davis-004, read as a whole, does not suggest the desirability of attesting an isolated execution mode, or proving validity of a program, or a configuration storage in a communication storage corresponding to an address space for an isolated execution mode. Ermolovich merely discloses status word in a command packet for a communication device, not a configuration storage for an isolated execution mode. Davis-986 merely discloses a BIOS upgrade, not a configuration of a device to exchange security information with a processor having a normal and isolated execution modes.

The Examiner failed to establish a prima facie case of obviousness and failed to show there is teaching, suggestion or motivation to combine the references. "When determining the patentability of a claimed invention which combined two known elements, 'the question is whether there is something in the prior art as a whole suggest the desirability, and thus the obviousness, of making the combination.'" In re Beattie, Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co., 730 F.2d 1452, 1462, 221 USPQ (BNA) 481, 488 (Fed. Cir. 1984). "To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or implicitly suggest the claimed invention or the Examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." Ex parte Clapp, 227 USPQ 972, 973. (Bd.Pat.App.&Inter. 1985).

In the present invention, the cited references do not expressly or implicitly suggest a digest memory, a device to attest isolated execution mode, or a configuration storage in a communication storage corresponding to an address space for an isolated execution mode. In

addition, the Examiner failed to present a convincing line of reasoning as to why a combination of Davis-004, Ermolovich and Davis-986 is an obvious application of attestation using an isolated digest and an isolated execution mode.

Therefore, Applicants believe that independent claims 1, 21, 41, 61 and their respective dependent claims are distinguishable over the cited prior art references. Accordingly, Applicants respectfully request the rejections under 35 U.S.C. §112, 35 U.S.C. §102(e), and 35 U.S.C. §103(a) be withdrawn.

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: July 27, 2004 By

Thinh V. Nguyen
Reg. No. 42,034
Tel.: (714) 557-3800 (Pacific Coast)

12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

☐ *deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.*

Date: July 27, 2004

FACSIMILE

☒ *transmitted by facsimile to the Patent and Trademark Office.*

Tu Nguyen July 27, 2004
Date